Attorney-General's Department

Public Consultation on Doxxing and Privacy Reforms

28 March 2024

By web form

Dear Attorney-General,

RE: Public Consultation on Doxxing and Privacy Reforms

EFA welcomes the opportunity to comment on the Australian Government's response and proposed legislative reforms to deal with the practice of 'doxxing'. EFA's submission is contained in the following pages.

EFA remains available to discuss our submission and the broader views of our organisation and members on this matter should the opportunity arise.

Yours sincerely,

John Pane
Chair
Electronic Frontiers Australia

About EFA

Established in January 1994, EFA is a national, membership-based, not-for-profit organisation that promotes and protects human rights in a digital context.

EFA is independent of government and commerce, and is funded by membership subscriptions and donations from individuals and organisations with an altruistic interest in promoting civil liberties in the digital context.

EFA members and supporters come from all parts of Australia and from diverse backgrounds. Our major objectives are to protect and promote the civil liberties of users of digital communications systems (such as the Internet) and of those affected by their use and to educate the community at large about the social, political, and civil liberties issues involved in the use of digital communications systems.

Electronic Frontiers Australia Inc.
ABN: 35 050 159 188
W www.efa.org.au
E john.pane@efa.org.au

Summary of Recommendations

EFA is significantly concerned by the rapid speed under which this consultation is being conducted. Doxxing has been a live issue well prior to the advent of Web 1.0 and 2.0, including the social media revolution starting in the early 2000s. This consultation is, to our mind, a knee jerk reaction by the government in response to, what we can reasonably infer, may be a vocal minority seeking to stifle and make lopsided public debate on the Israeli military action in Palestine. The problem of doxxing is broader, deeper, and more nuanced than it appears through this over simplified and reductionist lens.

In effect the government is allowing a little over **2 weeks** to collect feedback from Australian businesses, agencies, civil society organisations, academia and ordinary members of the public. Doxxing is an issue that is significant, complex and requires careful weighing, calibration, and consideration of a wide range of matters, some of which are conflicting. The implications of getting this law wrong are enormous.

1. **EFA's primary and overarching recommendations**:

- Entask the Australian Law Reform Commission ("**ALRC**") to lead a comprehensive review into doxxing. This would build upon work done in the **ALRC Serious Invasions of Privacy in the Digital Era Report** (ALRC Report 123), published in 2014 and made more contemporaneous from a technology, risk and harm perspective - Much has changed since 2014.
- Provide at least **3 months** for full public consultation by the ALRC including townhall or roundtable style meetings.
- Provide a **further 9 months** for the ALRC to conduct its analysis, undertake further clarifying round tables and town halls and provide the final report to the Government.

2. **EFA provides its qualified support, and with a significant degree of caution, to the expansion of the proposed statutory tort of privacy to cover doxxing.**

   Like defamation law, EFA holds strong concerns as to the availability of a remedy for doxxing under the proposed privacy tort as access to this type of legal remedy is often the exclusive domain of well funded and resourced, high net wealth individuals. It would be difficult for the average Australian, let alone those Australians that are disadvantaged in a variety of different ways, to access this legal remedy - it would be beyond their means, methods and knowledge.

   EFA holds the view that other statutory remedies are preferable. See 3 and 4 below.

3. No proposed changes to Privacy Act

Historically the ***Privacy Act 1988 (Cth***) (**'Act'**) was designed to regulate the processing of personal information by, in the first instance, Commonwealth agencies, subsequently ACT Government agencies and lastly, private sector organisations subject to a series of exceptions.

Arguably doxxing, if doner by an APP entity, may constitute a potential breach of Australian Privacy Principle (**'APP'**) 6 as an unauthorised use or disclosure of personal information by that APP Entity. This breach and potential offence however lacks specificity and particularity, making enforcement difficult. In addition, and certainly more critically, an individual who engages in doxxing in connection with their own personal, domestic or household affairs would be specifically exempted from the application of the Privacy Act by virtue of **Section 16 of the Privacy Act.**

A more specific remedy in carefully drafted legislation is required. See 4 below.

4. Amend the Criminal Code Act 1995 (Cth)

Under Section 474.17(1) of the ***Criminal Code 1995 (Cth)*** ("**the Code**"), a person commits an offence if they use a carriage service in a way that reasonable persons would regard as being, in all the circumstances, menacing, harassing or offensive.

Arguably, some but not all types of doxxing could be shoehorned into this provision but not without some difficulty, for example. "swatting". Swatting is a criminal harassment act of deceiving an emergency service (via such means as hoaxing an emergency services dispatcher) into sending a police or emergency service response team to another person's address. To illustrate the point further , s474.17 also requires modification to deal with 'deep fake' and related AI imagery (which is often pornographic) and which are now being used to harass, intimidate, demean, and ridicule people — in particular women, who are frequently the target of this type of criminal behaviour. EFA therefore does not fully support continued reliance upon Section 474.17(1) as a remedy for doxxing as it does not cover all of the different forms of doxxing and related risks and harms that might arise.

A person's reasonable expectation of privacy ought to be enjoyed by an individual beyond the current confines of the Privacy Act and Australian common law.

EFA believes it possible that s474.17 of the Criminal Code may be used to deal with a doxxing complaint in certain, limited circumstances only. The better view, and one that both reflects current technological capabilities and on-line behaviours, is to introduce a new provision in the Criminal Code, rooted in s474 but standing alone from s474.17 and designed **specifically** for doxxing and other associated on-line harms mentioned in this submission.

Introduction

Derived from the early hacker culture slang of ‘dropping docs [documents]’, doxxing is the intentional and malicious online exposure of an individual’s identity, private information, or personal details without their consent.

Revealing private information about a person without their consent for purposes of control, revenge, political discipline and attack, or silencing dissent is not new. The practice of revealing private information about individuals without their consent — known now as "doxxing" — has roots that extend deep into history, from the dissemination of personal details in Ancient Rome to concerns addressed by Justices Warren and Brandeis in their seminal 1890 work, "The Right to Privacy". In the modern era, the advent of the internet and subsequent technological advancements have significantly amplified the ease and scale at which personal information can be collected, stored, shared or weaponised. Online platforms have not only broadened the reach of individuals' networks but also asymmetrically enhanced their ability to harass, intimidate, or even attack others once private details are disclosed.

The emergence of doxxing in the 1990s found a powerful accelerant with the spread of Web 1.0 and 2.0 technologies, including the social media surge in the early 2000s. This period democratised technology and information access, transforming digital platforms into global public squares - but also created unique vectors for on-line and off-line personal harms.

In the intricate web of online interactions, doxxing emerges as a complex challenge. It's fueled by digital environments where algorithms enhance social division and turn shared opinions into weapons. This is partly due to ongoing practices of algorithmic behavioural manipulation by platforms and data aggregators, which foster polarisation and weaponization of shared ideas against those holding differing worldviews, as well as the recruitment of hostile strangers into domestic abuse situations.

Doxxing, along with the non-consensual sharing of intimate images, the creation of deep fakes, and the weaponisation of other emerging technologies, represents a broad category of digital and potentially real world harms that transcend traditional privacy and consent boundaries. These actions share the ability to harm in ways the victim may not directly witness, with the effects of doxxing and other digital abuses manifesting through the widespread dissemination of personal information or manipulated content. This dissemination leads to reputational damage, emotional distress, and physical threats, enduring well beyond the initial act of abuse.

Doxxing has the potential to serve as a force multiplier for other forms of harm. By exposing personal details, it can escalate existing or future threats, such as harassment or domestic violence, making it easier for perpetrators old or new to target victims.

This asymetric amplification of harm underscores the necessity for a comprehensive legal approach that encompasses not just doxxing, but all forms of digital abuse. For example,

doxxing may be inseparable from other forms of on-line or digital abuse, such as revenge porn, hacking and stalking and malicious deepfakes.

EFA's Preliminary Concerns

EFA is deeply concerned with the **extremely hasty manner** in which doxxing legislation consultations are being conducted. This approach fails to fully appreciate the multifaceted nature of doxxing and its intersection with other critical risks and harms, such as domestic violence laws and protective orders, revenge porn, hacking and stalking and malicious deep fakes.

The rush to enact doxxing-specific laws highlights a significant gap in the current legal framework to protect individuals adequately from a spectrum of digital harms, including harassment, intimidation, and breaches of privacy, particularly within domestic settings. A more deliberate and inclusive consultation process is essential to ensure that legislation effectively addresses the complex dynamics of doxxing and related digital abuses, offering comprehensive protection for individuals against these increasingly prevalent forms of harm.

EFA criticises the government's current approach to consultation as superficial, accusing it of failing to engage meaningfully and in good faith with civil society organisations, academia, and the public. The sidelining of domestic and family violence specialists and stakeholders is particularly alarming.

The current consultation process appears to be a mere formality, aimed at fulfilling basic legislative development requirements but in reality is a knee-jerk reaction to a highly publicised doxxing incident related to Israeli military action in Palestine. EFA argues that legislative reform, long overdue and much needed, should not be hastily enacted or used to cater to the interests of specific vocal lobby groups.

Background

Today's context

EFA is working with the definition that doxxing is the intentional online exposure of an individual's identity, private information, or personal details without their consent with the intention of exposing that individual to increased risk in digital and/or physical realms.

In the context of the current Israeli military action in Palestine, doxxing has affected both Zionist and pro-Palestinian communities and activists in Australia and abroad. The package of legislative reform, touted as a key measure to safeguard our online privacy and discourse, seems to be propelled forward more by the immediacy of these events and external pressures than by a comprehensive strategy to address the long neglected and nuanced challenges of the growing risks and harms of digital technologies operating within a patchy regulatory framework. To frame a response to this problem either solely through the lens of current Israeli military action, or in response to it, is both reductionist and simplistic.

The push for doxxing-specific legislation highlights a significant gap in the current legal framework's ability to protect individuals from individual or inter-connected digital harms, such as harassment, intimidation, and breaches of privacy, particularly in domestic settings. There is a need for a more thorough and inclusive consultation process around any new laws attempting to address the complex dynamics of doxxing and related digital abuses.

The social media phenomena of "call-out creators," who respect no international borders, serve as a stark example of how the inherently inter-jurisdictional nature of the internet complicates the drafting of effective doxxing legislation. Additionally, definitional issues surrounding terms like "harm" and "public" remain loosely defined, posing challenges to creating a standardised approach to legislating against a range of digital abuses that share underlying mechanisms of privacy invasion and psychological impact.

Recognizing the interconnected nature of digital abuses is essential. While acts such as doxxing, revenge porn, hacking, stalking, and the creation of malicious deepfakes may differ in their methods and specific impacts, they all involve the unauthorised use or dissemination of personal information or images with the intent to harass, intimidate, embarrass, or harm individuals. These acts collectively contribute to an unsafe online environment, undermining privacy, autonomy, and safety and often disproportionately affect women.

Legislation that addresses existing threats thoughtfully will be better prepared to handle emerging technological challenges. As technology evolves, new forms of digital abuse will arise, highlighting the need for adaptable and comprehensive legal frameworks. Effective legislation should anticipate and address future challenges, ensuring protection in a dynamic digital environment

What are the harms of doxxing?

Understanding the spectrum of risks and the potential or actual harms stemming from doxxing, and incorporating this understanding into effective legal frameworks, poses significant challenges. The variability of risks and harms related directly to or associated with doxxing — shaped by the victim's context, the nature of the doxxing, and ongoing debates within legal

scholarship over the definition of "harm" — highlights the complexity of addressing this issue through legislation. This complexity is further compounded by the subjective nature of assessing harm's impact, often leaving it to the victim to gauge the severity.

Doxxing manifests in various forms, each with distinct intentions and outcomes:

- **Deanonymizing Doxxing**: Reveals the true identity of someone who was previously anonymous or pseudonymous, compromising their privacy and safety.
- **Targeting Doxxing**: Shares specific information that allows others to contact, locate, or compromise the individual's online safety and security, such as revealing phone numbers, addresses, or login credentials.
- **Delegitimizing Doxxing**: Discloses sensitive or private information that can tarnish the individual's credibility or reputation, including medical records, legal documents, or private communications and photos.

It's crucial to distinguish doxxing from unintentional information sharing, whistleblowing, legitimate journalism, or releasing information in the public interest. Yet, the challenge lies in legislating intent and public interest — subjective concepts that vary widely in interpretation based on context and perspective.

Doxxing produces both first-order and second-order harms. The first-order harms of doxxing typically impact an individual's interests and/or bodily integrity directly and immediately, taking forms such as harassment or physical threats. It can also lead to second-order harms like job loss, reputational damage, and ongoing psychological distress, due to the enduring nature of online information ("the internet never forgets") and the (current) lack of a comprehensive data subject right of erasure or de-indexing. This permanence makes the doxxed information a tool for existing and future threats, as it remains accessible to be weaponized by new bad actors or exploited in unforeseen ways and prolonging the stigmatisation of the victim.

Doxxing is, further, a force multiplier for other threats and harms such as revenge porn, hacking and stalking and malicious deep fakes.

A force multiplier is a factor that dramatically increases the effectiveness of an action, making it significantly more impactful than it would be alone. As a force multiplier, doxxing not only causes direct harm through the invasion of privacy, it also expands the scale and severity of harassment an individual faces.

This amplification occurs in several key ways: it escalates existing harassment by providing harassers with more personal information; it facilitates new forms of abuse such as identity theft or stalking; it leads to a perpetual state of vulnerability due to the enduring availability of the information online; and, crucially, it exponentially increases the number of people engaged in the harassment. By turning personal details into weapons that can be used by a vast audience, doxxing multiplies the channels through which a victim can be targeted, escalating both the immediate and long-term risks they face.

When it is successful, doxxing is at its heart an isolation tactic that creates an acute social injury: it functions to remove individuals from the social or public spheres by depriving them of control over their level of personal exposure. This deprivation can lead to a forced withdrawal from public and community interactions, as victims seek to protect themselves from further exposure and the accompanying risks. This mechanism not only violates privacy but also disrupts the victim's ability to freely engage in social, professional, or civic life.

Further impacts of doxxing include:

- **Stripping Anonymity**: Anonymity enables individuals to express themselves, seek information, and participate in public discourse without fear of reprisal or judgement.
- **Delegitimising Individuals**: Reducing people to a single context, act, or belief creates a misleading impression with reputational consequences. In extreme cases it is dehumanising.
- **Chilling Free Expression**: Doxxing intimidates its victims into silence; but when used tactically it also carries an implied or explicit threat: that others who speak out will be similarly punished.
- **Undermining Digital Safety**: By weaponising the public sphere, doxxing undermines trust, community, and makes the digital environment less secure for everyone.
- **Interrupting Daily Life**: Affecting various aspects of personal life.
- **Concentrated Harm**: Disproportionately affecting women, children, and those already marginalised. Contexts like dating apps, family violence, and targeted campaigns .

Doxxing is a contributing factor to a range of recognized harms, including physical harm, public embarrassment, discrimination, cyber and physical stalking, identity theft, financial fraud, damage to personal and professional reputation, and psychological impacts like increased anxiety and diminished self-esteem.

EFA Recommendations

1. Privacy Tort

As part of the Attorney General's review and the Commonwealth Government's response to the Review of the Privacy Act a new statutory tort for serious invasions of privacy has been proposed. This proposal has been under discussion as a reform for the Privacy Act for two decades. Proposed to include a misuse of private information, this new statutory tort would allow individuals to seek redress through the courts if they have fallen victim to doxxing. Misuse of private information is a widely recognised type of invasion of privacy, already actionable in the UK, the US, New Zealand, Canada, and elsewhere.

As a remedy to doxxing, EFA offers its' qualified support to the proposed statutory tort as a remedy, as it would be difficult both in practical and financial terms for an ordinary Australian to bring such a matter to court. In addition, individuals who are vulnerable circumstances e.g. victims of domestic violence, sex workers etc, those in poor health, or otherwise disadvantaged would find it very difficult accessing this remedy.

To the extent that the Government creates a statutory tort of privacy which specifically deals with doxxing, EFA suggests the following principles constitute the essential elements and features of this remedy:

1. The invasion of privacy must be either by intrusion into seclusion or anonymity, or by misuse of private information;
2. It must be proved that a person in the position of the plaintiff would have had a reasonable expectation of privacy in all of the circumstances;
3. The invasion must have been committed intentionally or recklessly — mere negligence is not sufficient;
4. The invasion must be serious;
5. The invasion need not cause actual damage, and damages for emotional distress must be considered or awarded; and
6. The court must be satisfied that the public interest in privacy includes protected activities such as whistleblower protections and investigative journalism subject to an objective assessment of countervailing public interests.

2. No proposed amendment to the Privacy Act

Historically, the **Privacy Act 1988 (Cth)**, ('Act'), was designed to regulate the processing of personal information. Initially, it applied to Commonwealth agencies, then to ACT Government agencies, and finally to private sector organisations, all subject to a series of exceptions.

Of note, EFA refers to Section 16 of the Act which states:

16 Personal, family or household affairs

Nothing in the Australian Privacy Principles applies to:

(a) the collection, holding, use or disclosure of personal information by an individual; or

(b) personal information held by an individual;

only for the purposes of, or in connection with, his or her personal, family or household affairs.

The intent of this provision of the Act is evident in the Explanatory Memorandum to the ***Privacy (Private Sector) Amendment Bill 2000 (Cth)*** which provides:

> Clause 16E confirms that the National Privacy Principles do not apply to regulate the handling of personal information by an individual where that information is collected, held, used, disclosed or transferred for personal, family or household affairs (that is, done other than in the course of business). This is consistent with the exemption in sub-clause 7B(1)

This broad exception continues in existence today and would **still** apply in circumstances where an individual uses or discloses personal information in connection with their personal, family, or household affairs.

EFA does not support amending the Privacy Act to specifically capture doxxing because :

- The Act was designed to regulate the behaviour of Commonwealth and ACT Agencies and private sector organisations (subject to some exceptions) only and not individuals;
- APP entities engaging in doxxing would potentially, given the facts and the circumstances of the matter, be in breach of APP 6 but this lacks procedural certainty and is an ineffective remedy (as demonstrated in the Andie Fox vs Centrelink matter) ; and
- Individuals or incorporated or unincorporated entities engaging in doxxing should be covered by existing, compatible law, in particular **s417.17 of the Criminal Code Act 1995 (Cth).**

3. Amend the Criminal Code Act 1995 (Cth)

Under section 474.17(1) of the *Criminal Code 1995 (Cth)* ("**the Code**"), a person commits an offence if they use a carriage service in a way that reasonable persons would regard as being, in all the circumstances, menacing, harassing or offensive. The "service" can include a fixed or mobile telephone service, an internet service, or an intranet service.

The legislation stipulates that a person is guilty of an offence if:

1. the person uses a carriage service; and
2. the person does so in a way (whether by the method of use or the content of a communication, or both) that reasonable persons would regard as being, in all the circumstances, menacing, harassing or offensive.

EFA is of the view that while it is possible that s474.17 of the Code could be used to deal with certain types of doxxing complaints it is not fit for purpose in a broad range of situations as outlined in this submission. In addition, s474.17 as currently drafted does not provide a sufficient nexus with a person's reasonable expectation of privacy as ought to be enjoyed by an individual beyond the current operation and scope of the Privacy Act and Australian common law.

EFA believes the better view is to introduce a new provision in the Code, associated with s474 but standing alone from s474.17 and designed **specifically** for doxxing. EFA has drafted a preliminary model sub-clause to append to s474.17 below:

> A person (including a natural person, body corporate, or unincorporated entity) commits an offence if:
>
> (a) The person uses a carriage service to make an intentional online exposure of an individual's identity, private information, or personal details without their consent; and
> (b) The on-line disclosure was intentional or reckless; and
> (i) Was designed to harm an individual by intruding upon their seclusion, anonymity (in full or part), or their private affairs; or
> (ii) Constitutes public disclosure of private facts about an individual that may or has caused harm to them; or
> (iii) May place the individual in a false light to the public; or
> (iv) Appropriation of an individual's name and likeness.
> (c) This section does not apply if authorised by a relevant exception made under:
> (i) Section 7 of the *Privacy Act 1988 (Cth) or equivalent State or Territory Information Privacy law*;
> (ii) Applicable Commonwealth, State or Territory whistleblower protection legislation

Such an amendment, if adopted, will provide an effective deterrent and remedy for:

- Doxxing and other forms of on-line or digital abuse, such as:
- Revenge porn;
- Hacking and stalking; and

- Malicious deep fakes.